

COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD SUMMARY OF MEETING

**Microsoft Headquarters
Redmond, WA
December 4-6, 2000**

*Action items are highlighted in ***BOLD/ITALIC*** text.

Monday, December 4, 2000

Board Chairman, Franklin S. Reeder, convened the Computer System Security and Privacy Advisory Board meeting for its fourth meeting of the year at 1:40 p.m.

In addition to Chairman Reeder, Board members present were:

Mr. Peter Browne
Ms. Charisse Castagnoli
Mr. Richard Guida
Mr. Daniel Knauf
Mr. Stephen Lipner
Prof. George Trubow
Mr. James Wade
Ms. Karen Worstell

The entire meeting was open to the public. There was one member of the public in attendance when the meeting was called to order.

In the absence of Mr. Ed Roback, Dr. Fran Nielsen of NIST served as Board Secretariat for this meeting. Dr. Nielsen welcomed the newest Board Member, Charisse Castagnoli of Internet Security Systems, Inc. Dr. Nielsen then reviewed the meeting agenda and the handout materials provided to the members.

Chairman Reeder also welcomed Ms. Castagnoli as a member of the Board. He offered congratulations, on behalf of the Board, to Ed Roback on his recent appointment as the new Division Chief of the Computer Security Division at the National Institute of Standards and Technology (NIST). The other members of the Board expressed strong concurrence with those sentiments.

Discussion of Development of Principles and Values/Tenets

*Peter Brown and Dan Knauf
Discussion Leaders*

The purpose of this discussion was to develop a set of principles and roles/responsibilities that the Board could follow to communicate its positions to constituents. A focused platform for the Board to pursue based on the computer security and privacy mandates of the Board charter and the Computer Security Act of 1989 is needed. Mr. Brown shared some examples of First Union's information security principles and roles/responsibilities, and Mr. Knauf provided a set of examples of possible tenets for the Board's consideration. Following extensive discussion, the Board developed a draft list of potential issues to be considered. Topics on the list included:

governance and resources, IT acquisition and developments, intellectual property rights, and security; mining national security investments, mining the private sector best practices; resource allocation for information assurance (benchmarking); specific process management features/models; security metrics guidance, risk management guidance; development of a policy statement that includes a set of baseline standards, guidelines, and practices; establishment of criteria for privacy of data; and reexamination of the privacy Fair Information Practices.

The meeting was recessed for the day at 5:00 p.m.

Tuesday, December 5, 2000

Chairman Reeder reconvened the Board meeting at 9:15 a.m.

The minutes of the September Board meeting were reviewed and approved with minor edits. Board member, Mr Knauf, invited the members to attend the NSTISSC meeting being held at the Hunt Valley Marriott on April 3-5, 2001. ***Mr. Knauf will furnish additional details and meeting information.***

Review of the Computer Security Division Program

Tim Grance, NIST Computer Security Division

Tim Grance, Manager of the Systems and Network Security Group, presented an overview of the Computer Security Division program on behalf of Division Chief, Ed Roback, who could not attend. [Ref. 1] Mr. Grance covered the NIST mandate for computer security and the Division's mission. Key areas of the program include security standards, security testing, security research, assistance and guidance, and outreach. Mr. Grance said that there may be some restructuring within the Division pending the approval of the FY2001 budget. New security technologies that are being explored include the development of models, reference implementations, and demonstrations and transition of new technology and tools to public and private sectors. Examples of new technologies include authorization management, policy management, intrusion detection, and mobile agents. The Division assists U.S. government agencies and other users with technical security and management issues. Upcoming documents on PBX security, mobile code and active content, and telecommuting are being produced. Highlights for the year include the announcement of the Advanced Encryption Standard, the international Common Criteria Conference, federal PKI leadership, expansion of mutual recognition arrangements, and issuance of recent ITL Bulletins on mobile code, intrusion detection, and web server security.

For a future meeting, Chairman Reeder would like to hear a briefing from the Division on how the Division and NIST set their budget priorities.

The Center for Internet Security

Clint Kreitner, President/CEO

Mr. Clint Kreitner presented an overview of the Center for Internet Security. [ref. 2] The Center is a not-for-profit cooperative enterprise. The goal of the center is to provide methods to be used by organizations around the world to improve, measure, monitor and compare the security status of internet-connected systems and appliances, in order to effectively manage the organizational risks related to information security. The Center is establishing an Internet Appliance Testing and Evaluation Laboratory and creating an Internet Security Research Council. As of October 2000, the Center had an enrollment of 98 members. Members include government, industry, universities and foreign countries. Partners include the Information Systems Audit and Control Association (ISACA), the American Institute of Certified Public Accountants (AICPA), the Institute of Internal Auditors (IIA) and the SANS Institute. The Center has a membership fee structure to

cover individual professionals, user organizations, and information system security companies. Vendors will also be charged a fee to use the testing laboratory. The current focus of the Center is on benchmarks to create a common globally recognized basis for security status management and peer comparison and to provide methods that organizations can use to select and implement a level of security deemed appropriate in their risk management plan.

Mr. Kreitner welcomed any suggestions that the Board wished to offer.

Board Discussion on Congressman Horn's Computer Security Report Card

The Board discussed changes and additions to the earlier draft of a proposed letter the Board wants to send to Congressman Horn regarding his issuance of a report on federal agencies computer security programs. As a result of the Presidential election and changes occurring in the Administration, the Board offered several additional suggestions they believed would be important to the incoming transition team. ***Chairman Reeder will incorporate the changes and prepare the letter in final for forwarding to Congressman Horn.***

Legal and Policy Implications of the Gramm, Leach, Bliley (GLB) Act and the Health Insurance Portability and Accountability Act (HIPAA)

*Lee Zeichner, President
Legalnet Works, Inc.*

Mr. Lee Zeichner began his briefing by saying that the Board should get involved in the developments of the Gramm, Leach, Bliley (GLB) Act and Health Insurance Portability and Accountability Act (HIPAA) activities because of its significant information security policy activity and its fit within the Computer Security Act mission. He stated that the Board and NIST have relevant capabilities to contribute to the discussion of these issues. In his review of the GLB Act, he discussed the legal and policy methodologies, and the security and critical infrastructure protection issues. This Act's overarching framework affects not only federal agencies but also banking holding companies, utilities, national and international banking institutions, thrift and community banks, insured financial institutions, credit unions and brokers and dealers. Also included would be the uninsured and unregulated financial institutions and some States insurance industry.

The guidelines include specific security process requirements. These requirements include: Board of Director involvement; development of a written plan by CISO, a risk assessment identifying threats and vulnerabilities; physical protection focused on data; management of vendors who control access to system data; development of response and restoration programs; training and awareness for employees; and encryption of critical privacy data in storage and in transit.

Mr. Zeichner also reviewed other agency regulators decentralized policy approaches. He mentioned that the Securities and Exchange Commission will adopt a less specific approach and that the Federal Trade Commission is preparing safeguard rules that are expected to be complete in the upcoming months. The States are expected to remain silent on this issue.

Compliance penalties will be varied depending on the financial regulators. The statute focuses on financial regulators, the Securities and Exchange Commission and the Federal Trade Commission. The deadline for compliance has been set for July 2001 and the agencies will be responsible for audits and enforcement of compliance.

The roots of HIPAA are simplification, uniformity and consistency. Congress has required the Department of Health and Human Services (HHS) to implement the standards development provisions of the Act. The HHS is preparing a series of proposed rules that will apply principally

to the health care community. These rules reflect largely technical requirements that are sophisticated, extensive and process oriented.

Penalties for non-compliance with HIPAA are severe and could include imprisonment and civil fines. The requirements are specific and mandatory in contrast with GLB, where compliance with the requirements is not as prescriptively described by the statute but will be more driven by agency regulations and judicial interpretation. Compliance and enforcement will be linked to the size of the operation for the first several years. At present, it is unclear who will audit or enforce on-scene compliance. Separate information security and privacy rules are being developed, but have not yet been released.

Mr. Zeichner recommended that the Board closely track GLB and HIPAA developments. The capability that NIST offers and the dialogue that it can generate, especially related to the privacy issues, can be a benefit. The Board could help ensure that the relationship between some of the issues can be more understood among agencies. Mr. Zeichner also said that the Board should provide comments on some of the regulations that are being developed and he encouraged them to also provide their findings to the Office of Management and Budget.

Mr. Reeder thanked Mr. Zeichner for his insightful briefing on these two important topics and said that the Board would be following these issues very closely.

Privacy Event Planning

*Rick Weingarten
George Trubow*

Mr. Weingarten and Professor Trubow discussed the proposed privacy event the Board plans to hold in conjunction with the June Board meeting. A proposed topic for this event is to hold a moot court on federal agencies using cookies in Internet transactions with individuals. Board members would participate as judges. Professor Trubow offered to have a team of his students participate to argue the case. He also said that he would check on the possibility of holding this event at the John Marshall Law School in Chicago, IL. After further discussion, it was decided that the moot court exercise would serve as the centerpiece for a larger privacy event with a list of briefings that could include GPEA panels, GLB-HIPAA, and the impact of these Acts on the Social Security Administration and the Internal Revenue Service. George Trubow, Rick Weingarten and Charisse Castagnoli will serve as the program committee. ***Board members should be in touch with the program committee regarding any additional suggested topic areas.***

Public Participation

There were no requests for public participation at this meeting.

The Chairman recessed the meeting at 3:30 p.m.

Wednesday, December 6, 2000

The Chairman resumed the meeting at 8:45 a.m.

Board Discussion on Work Plan

A straw vote was taken on the specific tasks that the Board had previously identified. The list was reviewed and, based on criteria established by the Board, the list was reduced to six major

target areas. The Board is to develop a one-to-two page statement for each area. The statement should define specific objectives, activities, resources, and partners that would be needed for the Board to have an impact on the respective issue. Each statement should also include a proposed time line for pursuing these work objectives. Below is the list of target areas and their working group.

- Governance – Peter Browne, Rich Guida, Dan Knauf, Jim Wade,
- Best Practices – Steve Lipner, Fran Nielsen, John Sabo
- GPEA Process – Rich Guida, Jim Wade, Rick Weingarten
- Security Metrics – Peter Browne, Fran Nielsen, Frank Reeder,
- Privacy – Charisse Castagnoli, Rich Guida, Fran Nielsen, George Trubow, Rick Weingarten, John Sabo
- Baseline Standards – Steve Lipner, Karen Worstell, John Sabo

These statements should be circulated to the Board members for their review and discussion at the March Board meeting.

Security Metrics and Open Forum Discussion

*Steve Lipner
Fran Nielsen*

Dr. Nielsen reported that she had not received any comments or suggestions for change to her security metrics workshop report; therefore, it was finalized and added to the Board website.

Mr. Lipner observed that what the General Accounting Office (GAO) was doing in security metrics appeared to be successful, and he asked if NIST was working with them to promulgate this effort. Dr. Nielsen indicated that NIST was working with GAO in its efforts to develop the security framework document. Also, the efforts of the Center for Internet Security will address security metrics issues.

The security metrics workshop opened up dialogue between NIST and some of the attendees that was very beneficial, reported Dr. Nielsen. Members of the Board commented that the models presented during the workshop were very good and useful to them. The Board felt it would be useful to have a comparative analysis done on each model that was presented. It would also be useful to revisit the presenters at the workshop and ask them if there is anything else that the Board could do to advance the state of measurement. ***Dr. Nielsen has the action to produce a metrics taxonomy as well as to develop a process proposal to further the dialogue on this issue through periodic face-to-face meetings, electronically convening forums, reference tool developments, etc.***

Development of Agenda Topics for March 2001 Meeting

The following is a list of suggested actions for the March 2001 meeting.

1. One day to be devoted to the presentation and discussion of the work plan proposals.
2. OMB briefing on the Thompson-Lieberman Act as enacted and the OMB guidance that is to be produced as a result of this legislation.
3. In-depth briefing of the Computer Security Division and its budget for 2001.
4. Briefings to Administration transition teams on how the Board could sensitize incoming officials on computer security and privacy issues

5. Update on the Public Key Infrastructure initiative by GSA.
6. Briefings on digital risk management from NIST and the private sector including the film and recording industry. Intellectual property rights issues should be included in the briefing.

Action items from this meeting are listed below.

1. Dan Knauf is to furnish detailed meeting information about the April 3-5, 2001, meeting of the NSTISSC being held at the Hunt Valley Marriott in Baltimore, MD.
2. Chairman Reeder is to take the Board's suggested changes and finalize the letter to Congressman Horn.
3. Fran Nielsen is to produce a metrics taxonomy as well as develop a process proposal to further the dialogue on the metrics issue through periodic face-to-face meetings, electronically convening forums, reference tool developments, etc.
4. Board members should contact Charisse Castagnoli, George Trubow or Rick Weingarten if they have any additional suggested topics for the June privacy event.
5. The work plan statements should be circulated to the Board members for their review and discussion at the March Board meeting.

There being no further business, the meeting was adjourned at 10:50 a.m.

Ref.1 Grance presentation
Ref. 2. Kreitner presentation
Ref. 3 Zeichner presentation

Edward Roback
Board Secretary

CERTIFIED as a true and accurate
summary of the meeting.

Franklin S. Reeder
Chairman